

FILED

08 JAN -7 AM 9:58

CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

BY:

DEPUTY

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,

v.

RICHARD SILLS, JR.,

Defendant.

No.

'08 MJ 0037

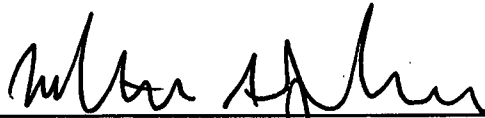
COMPLAINT FOR VIOLATION OF

Title 18, U.S.C., Sec. 1038 -- False
Information and Hoaxes

The complainant being duly sworn states that:

On or about December 5, 2007, within the Southern District of California, defendant RICHARD SILLS, JR., engaged in conduct with intent to convey false or misleading information under circumstances where such information may reasonably be believed and where such information indicates that an activity has taken, is taking, or will take place that would constitute a violation of perpetrating hoax devices, all in violation of 18 USC 1038.

This complaint is based on the attached affidavit, incorporated herein.


HEATHER A. JACKSON, Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me on January 4, 2008.


UNITED STATES MAGISTRATE JUDGE

CATHY ANN BENCIVENGO
U.S. MAGISTRATE JUDGE

AFFIDAVIT IN SUPPORT OF COMPLAINT

I, Heather A. Jackson, being first duly sworn, declares and states that:

INTRODUCTION

1. I am the Affiant herein, and that I am a Special Agent with the Federal Bureau of Investigation (FBI), assigned to a FBI Counter Terrorism Squad, having been employed by the FBI for approximately four (4) years. The following information was obtained by the Affiant and other law enforcement personnel.

2. For the past two years the Affiant has worked on a terrorism squad focusing primarily on domestic terrorism. The Affiant has received various training on domestic and international terrorism groups. The Affiant has also been the case agent in multiple FBI domestic terrorism investigations. I submit that the facts contained in the numbered paragraphs below demonstrate that there is probable cause to believe that fruits, instrumentalities, and evidence of violations of Title 18, U.S.C. 1038 (perpetration of hoaxes) will be found at the three following locations:

- (1) University of California at San Diego (UCSD), Biomedical Sciences Building, Second Floor, Room 2082 and 2080, La Jolla, California, 92093; (hereinafter referred to as "Target Location 1")
- (2) 924 Encinitas Boulevard, Apartment 111, Encinitas, California 92024 (hereinafter referred to as "Target Location 2");
- (3) 1998 Subaru Outback, California license plate 4STV626, VIN JF1GF4854WG03727 (hereinafter referred to as "Target Location 3").

Target locations 1, 2, and 3 are further described in Attachment A, which I hereby incorporate by reference.

3. The evidence to be searched for and seized is listed in Attachment B to the applicable search warrant application, incorporated herein.

//

BASIS FOR THE FACTS CONTAINED IN THIS AFFIDAVIT

- 1
- 2 4. I make this affidavit, in part, based on personal knowledge derived from my
- 3 participation in this investigation and, in part based upon information from the following sources:
- 4 a. oral and written reports about this investigation and others that I have received
- 5 from Detectives and Special Agents of the FBI, San Diego Police Department,
- 6 Metro Arson Strike Team (MAST), and UCSD Police Department.
- 7 b. physical surveillance conducted by federal agents or local law enforcement agents
- 8 wherein observations have been reported to me either directly or indirectly.
- 9 c. witness interviews conducted by federal agents or local law enforcement agents,
- 10 wherein interviews were conducted by me or reported to me.
- 11 5. Since this affidavit is being submitted for the limited purpose of securing court
- 12 authorization for a search warrant to locate and seize fruits, instrumentalities, and evidence of
- 13 perpetration of hoaxes, I have not set forth each and every fact learned during the course of the
- 14 investigation. Nor have I summarized each and every factual circumstance deemed to be pertinent
- 15 to the case. Rather, I have set forth only those facts that I believe are necessary to establish
- 16 probably cause for the requested search warrant.

17 **FACTS AND CIRCUMSTANCES ESTABLISHING PROBABLE CAUSE**

18 **A. INVESTIGATION OVERVIEW**

19 6. On December 5, 2007 a hoax improvised explosive device (IED) was discovered

20 at the Leichtag Biomedical Research Building (LBRB) located on University of California at San

21 Diego (UCSD) campus. Prior to the discovery, four phone calls were placed warning of drastic

22 action against medical buildings at UCSD as well as a letter claiming that explosive devices had

23 been placed in several buildings including the "Leichstad [sic] Research Building." The San

24 Diego FBI sent the original threat letter to the FBI Laboratory Division in Quantico, Virginia for

25 forensic analysis.

26 //

1 7. Based on subpoenaed toll records, three of the four phone calls warning of this
2 drastic action originated from the cellular phone number of 858-877-0663 (**Telephone #1**). The
3 subscriber of this phone number is Richard SILLS, Jr, social security account number 564-XX-
4 XXXX. The UCSD police department confirmed that a Richard SILLS with the same social
5 security account number is currently employed at UCSD as a temporary administrative assistant.
6 SILLS has been working as the administrative assistant to John Rice Kelsoe, Jr., since August 27,
7 2007. Kelsoe's office is located in the Biomedical Science Building (BSB), Room 2080 and Room
8 2082 and he confirmed that SILLS works for him as his administrative assistant in the same
9 workspace. The BSB is located across a small courtyard from the LBRB, the building where the
10 hoax IED was found.

11 **B. BACKGROUND ON Richard Craig SILLS, Jr**

12 8. Richard Craig SILLS, Jr, date of birth November 11, 1953, social security account
13 number 564-XX-XXXX, has been employed at UCSD since August 8, 2006 as a temporary
14 administrative assistant. SILLS has been working as an administrative assistant for John Rice
15 Kelsoe, Jr. since August 27, 2007. SILLS works in the Biomedical Sciences Building, in room
16 2082. SILLS's office area is adjacent to the office of Kelsoe, room 2080, and he has access to both
17 rooms. The two offices are connected by an internal doorway.

18 9. On January 2, 2008, at approximately 12:15 p.m., SA Louis D. Hillyard observed
19 SILLS exiting room 2082 and locking the door behind him with a key.

20 10. Richard SILLS is the subscriber for a Verizon Wireless cellular phone number
21 858-877-0663. The billing address for his phone bill is 924 Encinitas Boulevard, Apartment 111,
22 Encinitas, California, 92024. On January 2, 2008, SA John Farr observed SILLS leaving work
23 from UCSD and driving a dark black 1998 Subaru Outback, California license plate 4STV626.
24 SILLS drove to 924 Encinitas Boulevard, Building #14, Apartment 111, Encinitas, California,
25 92024 and parked the vehicle in carport number 67. SILLS entered Apartment 111 with a key.
26 According to California Department of Motor Vehicles (DMV) records, SILLS is the registered

1 owner of a 1998 Subaru, California license plate 4STV626.

2 **C. PROBABLE CAUSE**

3 11. At approximately 10:15 a.m., on December 4, 2007 John Van Zante, Public
4 Relations Manager for the Helen Woodward Animal Center received an anonymous voice message
5 from a male caller stating the following: "John, you need to know that the American Animal
6 Liberation Front is going to be doing a very drastic action against UCSD animal torture facilities in
7 the medical schools and research centers. That's happening today. They have been told they need
8 to take all the animals to a central animal location and a sanctuary would be there to help them
9 relocate those animals. If not, there's going to be extreme consequences. So, I'm giving you a
10 heads-up. Hopefully you all will be there."

11 12. At approximately 8:45 a.m., on December 5, 2007, UCSD's Office of Research
12 Affairs received an anonymous call from a male caller stating the following: "You need to take
13 this very seriously -- there is a bomb in Leichtag."

14 13. At approximately 9:05 a.m., on December 5, 2007, UCSD's Chancellor's Office
15 received an anonymous call from a male caller stating the following: "Take this very seriously,
16 there is a bomb in the Leichtag building, take this very seriously."

17 14. On December 5, 2007 between 8:00 a.m. and 9:00 a.m., the UCSD police
18 department received a letter sent through inter-campus mail and signed by "A.L.F.". The first two
19 lines of the typed letter read (in all capital letters), "WARNING! WE REPRESENT THE
20 ANIMAL LIBERATION FRONT." The letter also threatened "VERY DRASTIC ACTION ON
21 UCSD MEDICAL SCHOOL AND RESEARCH FACILITIES." The letter claimed that the action
22 had been planned for a long period of time and that they had the capability to execute the plan.
23 The letter further threaten that a remote controlled explosive devices had been placed in six
24 buildings at UCSD, to include the "Leichtag [sic] Research Building," and possibly more
25 locations. The letter continued on to say that if "THEY" did not see the evacuation of animals by
26 3:00 PM on December 4, 2007, "THEY WILL DETONATE REMOTELY ALL EXPLOSIVE

1 DEVICES." This threat letter was collected from UCSD police department by the San Diego FBI
2 and placed into evidence on December 5, 2007. On December 6, 2007, this letter was sent to the
3 FBI Laboratory Division for forensic analysis.

4 15. On December 5, 2007 at approximately 10:26 a.m., Shirley Reynolds, Lab
5 Manager at the Leichtag Biomedical Research Building, called the UCSD police department to
6 report the discovery of a suspicious device found in the LBRB. Initial analysis of the device by
7 FBI Special Agent (and bomb technician), James G. Verdi was conducted at approximately 11:00
8 a.m. on December 5, 2007. SA Verdi observed what appeared to be an antenna attached to the
9 device. Based on the threat of remote detonations, the presence of this antenna increased concern
10 that this was a functional IED.

11 16. As a result of the discovery of this device, the UCSD police department in
12 conjunction with the San Diego Police Department evacuated the LBRB and several neighboring
13 buildings. At approximately 3:30 p.m., the Metro Arson Strike Team (MAST) further examined
14 and x-rayed the device and determined the device to be a hoax IED.

15 17. The hoax IED is a 1.02 pound Coleman camping fuel cylinder (presumed empty)
16 with four 12-gauge shotgun shells taped to the outside of the cylinder with yellow masking tape.
17 Additionally, wires with audio plugs were also taped to the fuel cylinder along with what appears
18 to be a television antenna and cable. The hoax IED was contained inside a plastic "Henry's"
19 grocery bag. The hoax IED and grocery bag were place into FBI evidence on December 5, 2007
20 and also sent to the FBI Laboratory on December 6, 2007.

21 18. On January 2, 2008, law enforcement personnel observed SILLS at his place of
22 work, Room 2082, BSB, University of California, San Diego.

23 19. On the morning of January 3, 2008, Special Agents conducting surveillance
24 observed SILLS exit his vehicle, the 1998 Subaru, California license plate 4STV626 in a parking
25 lot at the University of California, San Diego. Subsequent observation of SILLS's vehicle revealed
26 two suitcases located in the backseat area of the vehicle.

1 20. Forensic analysis conducted by the FBI Laboratory, Trace Evidence Unit,
2 determined that there were textile fibers of different types and colors found on the hoax IED, the
3 plastic bag, and the threat letter.

4 21. The FBI Laboratory submitted the threat letter to the United States Secret Service
5 (USSS), Forensic Services Division, for color toner coding examinations. The color toner
6 examinations determined that the letter was printed from a Hewlett Packard Color Laser Jet 4700,
7 serial number JP4LD02904. The USSS was also able to determine that this printer was sold and
8 shipped on October 22, 2007 to the following address: "University of California, BSB 2082, La
9 Jolla, CA, 92093-0000, USA." The USSS Forensic Services Division explained that documents
10 produced on these types of printing systems can contain encoded information that may reveal the
11 serial number and location of a given printer. Such information was located on the threat letter
12 received by the UCSD Police Department on December 5, 2007. The UCSD Police Department
13 confirmed that "BSB" refers to the UCSD Biomedical Sciences Building.

14 22. On January 3, 2008, the Affiant and Special Agent Matthew Perkins interviewed
15 Dr. John Kelsoe. Kelsoe confirmed that the printer in Room 2082, which is used by Kelsoe and
16 SILLS, is an HP Color Laser Jet 4700, unit serial number JP4LD02904. Kelsoe further confirmed
17 that SILLS has access to print from the printer located in his office and gave consent for agents to
18 search his office. According to Kelsoe, in his 10 years experience in this office, no one other than
19 himself and his administrative assistant have printed to the printer located in Room 2082.

20 23. Kelsoe stated that SILLS is the administrative assistant to Dr. Kelsoe, a Professor
21 of Psychiatry at UCSD. Kelsoe stated that SILLS has been working for him since late August of
22 2007.

23 24. Kelsoe further stated that SILLS occupies Room 2082, and he (Kelsoe) occupies
24 Room 2080, which is adjoined to Room 2082 by an internal entranceway that remains open at all
25 times. Kelsoe stated that both rooms have doors that lead to the west hallway of the BSB, but only
26 the door to Room 2082 is used to enter the offices. The door to Room 2080 remains locked from

1 the hallway at all times. Kelsoe stated that the only people have access to Room 2082: himself,
2 SILLS, a third individual who works as the department's Information Technology administrator,
3 and the cleaning staff.

4 25. Kelsoe further stated that both he and SILLS have their own desktop computers.
5 Kelsoe believed that there are also two external servers that are accessible from those computers.

6 26. Agents played for Kelsoe a recording of a call made to the U.S. Attorney's Office
7 for the Southern District of California on December 13, 2007 from an anonymous caller who
8 claimed to be responsible for the hoax bomb. Kelsoe stated that he did not recognize the voice.

9 27. On January 4, 2008, agents executed court-authorized search warrants of SILLS's
10 residence, 924 Encinitas Boulevard, Apartment 111, Encinitas, California 92024. Agents found
11 the following items:

- 12 a. A piece of paper with the name of Assistant U.S. Attorney (AUSA) Michael
13 Skerlos and the address of the United States Attorney's Office. AUSA Skerlos is
14 one of the attorneys working on this investigation to date.
- 15 b. A piece of paper with the main telephone number for the United States Attorney's
16 Office for the Southern District of California, the telephone number for the FBI's
17 San Diego's office, and the name and telephone number of "Jason Sur [sic]," a
18 defense attorney employed at Federal Defender's, Inc. who has also been involved
19 in this case.
- 20 c. A piece of paper with the name and telephone number of AUSA Skerlos. On the
21 same piece of paper is the name and telephone number of Jodi Thorp, a private
22 defense attorney in San Diego.
- 23 d. A box of 12-gauge shotgun shells that are identical to the shotgun shells attached
24 to the hoax device on December 5, 2007. Eight shotgun shells were missing from
25 the box. Four were found in a shotgun located at the residence. The hoax device
26 found on December 5, 2007 had four shotgun shells attached to it.

- 1 e. A Coleman camping fuel tank. The Coleman fuel tank is identical to the Coleman
2 fuel tank that was used as the hoax device found on December 5, 2007.

3 **TELEPHONE SUBSCRIBER INFORMATION AND TOLL ANALYSIS**

4 28. On December 13, 2007, Grand Jury subpoenas for telephone subscriber
5 information and for toll analysis for telephone number (858) 877-0663 ("**Telephone #1**") was
6 issued to Verizon Wireless. Records produced by Verizon Wireless indicated that **Telephone #1**
7 is subscribed to by Richard SILLS, Jr. of 924 Encinitas Boulevard, Apartment 111, Encinitas,
8 California 92024.

9 29. Telephone toll analysis of **Telephone #1** indicated that **Telephone #1** placed a
10 call at 10:14 a.m. on December 4, 2007 to (858) 756-4117, the number for the Helen Woodward
11 Animal Center located in Rancho Santa Fe, California.

12 30. Telephone toll analysis of **Telephone #1** indicated that **Telephone #1** placed a
13 call at 10:39 a.m., on December 4, 2007, to (858) 571-8888, the number for KFMB TV Channel
14 Eight, a San Diego television station.

15 31. Telephone toll analysis of **Telephone #1** indicated that **Telephone #1** placed a
16 call at 10:40 a.m., on December 4, 2007, to (858) 650-5401, the number for Fox6, XETV Channel
17 Six, a San Diego television station.

18 32. Telephone toll analysis of **Telephone #1** indicated that **Telephone #1** placed a
19 call at 8:45 a.m., on December 5, 2007, to (858) 534-3526, the number for Arthur B. Ellis, UCSD's
20 Vice Chancellor for Research. According to Ellis, he is also the Institutional Official for UCSD's
21 biomedical research program.

22 33. Telephone toll analysis of **Telephone #1** indicated that **Telephone #1** placed a
23 call at 9:06 a.m., on December 5, 2007, to (858) 534-3135, the number for the Office of the
24 Chancellor at UCSD.

25 34. Telephone toll analysis of **Telephone #1** indicated that **Telephone #1** placed a
26 call at 3:15 p.m., on December 12, 2007, to (619) 338-4700, the number for the Public Defender's

1 Office. Subsequent to this call, an anonymous caller claiming responsibility for the hoax bombing
2 incident called Steven Barth of Federal Defenders, Inc. Barth is appointed counsel for a different
3 individual who was previously charged in relationship to this crime.

4 35. Telephone toll analysis of **Telephone #1** indicated that **Telephone #1** placed a
5 call at 1:36 p.m., on December 13, 2007, to (619) 542-4586, the telephone number for Greg
6 Moran, Staff Reporter for the San Diego Union-Tribune. Moran is a Union-Tribune reporter
7 covering the hoax bombing case. Moran wrote two articles regarding the hoax bomb case on
8 December 10, 2007, and a third article on December 11, 2007. All three articles appeared on the
9 Union-Tribune's website.

10 36. Telephone toll analysis of **Telephone #1** indicated that **Telephone #1** placed a
11 call at 2:51 p.m., on December 13, 2007, to (619) 557-5610, the number for the United States
12 Attorney's Office for the Southern District of California. At 2:53 p.m., a message was left at the
13 U.S. Attorney's Office by a male caller who identified himself as "A.L.F.," and described the hoax
14 bomb in great detail. The caller concluded by saying "The person who put it together would know
15
16 that, that was me." Calls made to the U.S. Attorney's main number are received by an automated
17 answering system that can direct calls to a specific individual's office by prompting the caller to
18 key in the individual's name.

19 **DIGITAL EVIDENCE**

20 37. Based upon information related to me on December 30, 2007, by Craig Porter of
21 the San Diego Regional Computer Forensics Laboratory (SDRCFL), I know that digital evidence
22 can be stored on a variety of systems and magnetic, optical and mechanical storage devices
23 including, but not limited to, hard disk drives, floppy disks, CD-ROMs, DVD-ROMs, magnetic
24 tapes, magneto optical cartridges, personal digital assistants, pagers and memory chips.

25 38. SA Craig Porter, a Computer Forensic Examiners (CFE) of the SDRCFL, has
26 instructed me on the proper manner in which to safely transport any seized digital media to a

1 secure Evidence Storage Facility.

2 39. Any computers or computer systems, as defined in Attachment "B", found at
3 Target Locations 1, 2, or 3 may be seized, transported from the scene, imaged at the SDRCL, and
4 examined. This procedure is justified for two reasons. First, as set forth above, there is sufficient
5 probable cause to show the Court that the computers and computer systems contain contraband,
6 constitute evidence of the commission of a criminal offense, and/or were used as the means of
7 committing a criminal offense.

8 40. Second, searching computers and computer systems is a highly technical process
9 that requires specific expertise, equipment and software. There are a multitude of different types
10 of computers manufactured today, many of which use proprietary hardware and software during
11 the creation of any user data. It is impracticable for the law enforcement community to have all
12 the proper adapters, cables, cords and other hardware devices necessary to consistently link law
13 enforcement forensic equipment with all known and unknown computer systems on an immediate
14 basis while searching "on-site." Much of this specialized equipment is available, but may need to
15 be acquired in order to conduct a proper forensic examination.

16 41. There are literally thousands of different software programs that can be
17 commercially purchased and installed on a user's computer system. As computer security has
18 become an ever-increasing priority to many consumers, much of today's commercially available
19 software is developed for, or provides, data security and encryption which makes it difficult to
20 afford an accurate representation of any digital evidence confronted with on-site. Moreover, it is
21 feasible for a Computer Forensic Examiner to be familiar with every software program, past or
22 present, now commercially available. It may be necessary for a CFE to train with a particular type
23 of software in order to fully understand the capabilities of that software.

24 42. In order to safeguard the integrity of a computer forensic examination, it is
25 imperative that the CFE first make a complete image of the original digital evidence before
26 conducting a forensic examination. The CFE must ensure that any images made are forensically

1 sound and that these forensic images can be fully restored, if necessary. There are numerous
2 pitfalls that can seriously hamper the integrity of the imaging process while on-site. For example,
3 to make a forensically sound image of targeted original digital evidence, the CFE must ensure that
4 there is an adequate uninterruptible power supply. Digital evidence is extremely fragile and
5 susceptible to power interruptions or power surges. It is not always practical for a CFE to bring
6 backup power supplies into the field.

7 43. Additionally, it may be necessary for the CFE to have unrestricted access to the
8 original digital evidence during the course and scope of the forensic examination. There are
9 numerous operating systems now being used by consumers. Some of these operating systems
10 include, but are not limited to, DOS, Windows 3x, Windows 9x, Windows NT, Windows 2000,
11 Macintosh, Linux, Unix, Novell and PICK. These operating systems use different file structures,
12 different partition formatting and different file commands. Moreover, many of these operating
13 systems are "hardware" specific. This means that a restored image of original digital evidence may
14 not be "bootable" or "viewable" without the actual original hardware. This would prevent the CFE
15 from viewing the restored digital image in a manner consistent with the structure of the original
16 digital evidence. This problem is especially acute when dealing with operating systems like Linux,
17 Unix, MAC and Novell.

18 44. These problems are accentuated by the fact that it is possible for a user to have
19 two or more different operating systems on the same piece of original digital evidence. This
20 severely hampers the CFE's ability to image this type of original digital evidence on-site due to
21 certain software limitations. This type of problem generally requires that the imaging process take
22 place in a controlled environment, such as the SDRCFL. Once this procedure is completed, a CFE
23 can then safely conduct most types of requested examinations using this newly created "image" file
24 without fear of damaging, destroying, adding or altering any files or operating system components
25 of the original digital evidence.

26 //

1 45. It is also very difficult in today's computer environment to "search" for specific
2 data while on-site. To conduct any type of digital "search" without using a forensically created
3 image predisposes multiple forensic problems. It may literally take hours, if not days, to
4 appropriately search a medium to large size hard drive for any desired data. For example, a search
5 for the word "kill" during a homicide investigation could find thousands of positive hits, due to the
6 fact that while a subject may have in fact wanted to kill the victim, the term "kill" is also a valid
7 computer command related to the ending of an otherwise innocuous computer process.

8 46. Computers can be difficult to examine even if no serious effort is used to conceal
9 or protect its digital contents. A complete forensic search is not limited to examining files
10 normally displayed by the operating system. It also includes the expansion of compressed data and
11 the recovery of deleted file data. It involves the areas on a computer hard drive that the computer
12 system recognizes as being "in use" and those areas that the computer system deems "available for
13 use." This search may involve an examination of "slack" space, which is the information at the
14 end of a sector or cluster beyond the end of the "current" usage. Finally, the complete examination
15 would address "orphaned" data, portions of files left behind by earlier operating system activity.
16 All of these areas require operating specific tools and techniques to access the data.

17 47. It is also very easy for a computer user to conceal data or other types of digital
18 evidence through a number of methods, including the use of innocuous or misleading filenames
19 and extensions. For example, files with the extension ".jpg" are digital image files. A moderately
20 sophisticated computer user, however, can easily change the .jpg file extension to ".txt" or ".dll" in
21 order to conceal or mislead law enforcement into thinking the digital image is actually a text or
22 system file. While it may be possible for a CFE to notice this during a properly controlled forensic
23 examination, it is difficult for that same CFE to detect this concealment during an on-site
24 examination. For example, the Windows 9x Operating System, installed right out of the box,
25 would itself contain over 20,000 different system files. A devious user could then alter any
26 improper files so as to make them appear to be legitimate files.

1 48. The problems noted above are compounded by the fact that the volume of data
2 stored on a typical computer system is so large that it would be unrealistic to search for specific
3 data while conducting an on-site examination. For example, a single megabyte of storage space is
4 the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000
5 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are
6 now capable of storing more than 60 gigabytes of data and are commonplace in new desktop
7 computers.

8 49. Additional problems are created by the growing use of destructive programs or
9 "booby traps." These programs can destroy or alter data if certain forensic procedures are not
10 scrupulously followed. Since digital evidence is particularly vulnerable to inadvertent or
11 intentional modifications or destruction, a controlled environment, such as the SDR CFL, is
12 essential to conducting a complete and accurate examination of any digital evidence. This
13 problem mandates that all examinations need to take place using only a forensic image of the
14 original digital evidence.

15 50. Finally, there is also a growing use of military-grade encryption by consumer and
16 commercial computer users. These encryption programs, which are low or no cost, are widely
17 available and allow users to encrypt specific data with just a few keystrokes. These encryption
18 problems are accentuated by other newer technologies, like steganography, which allows a user to
19 conceal information within other files. It is difficult to detect the use of this technology without a
20 proper forensic examination and the ability to look at the entire image of the subject digital
21 evidence.

22 //

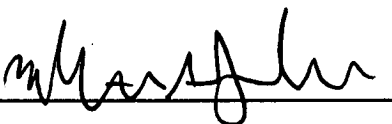
23 //

24 //

25 //

26 //

1 51. For the reasons set forth above, I respectfully request that I be allowed to seize all
2 computers and computer systems, as defined in Attachment "B," and transport them to the
3 SDRCFL for a proper forensic examination including imaging and searching.

4
5 

6 Heather A. Jackson, Special Agent
7 Federal Bureau of Investigation

8 **SUBSCRIBED** and **SWORN** to before me,
9 this 4th day of January, 2008

10 
11 UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

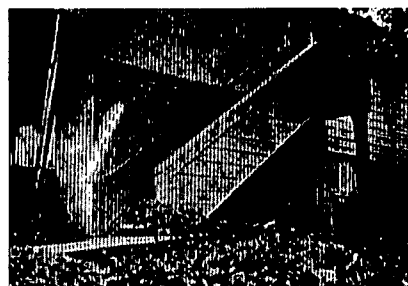
SUBJECT PREMISES

Based on the information set forth below, the Affiant believes there is probable cause that certain items, described below in Attachment B, will be found at the following described premises:

1. **University of California at San Diego (UCSD), Biomedical Sciences Building, Second Floor, Room 2080 and 2082, La Jolla, California, 92093 ("Target Location 1").**

Target Location 1 is located in office space designated as Rooms 2080 and 2082 on the second floor of the Biomedical Sciences Building at the University of California's San Diego campus in La Jolla, California 92093. The two rooms are adjoined by an internal entrance way. Both Room 2080 and Room 2082 have separate entrance ways from the west hallway of the Biomedical Sciences Building, although it is not possible to gain access to Room 2080 from the hallway. The entrance into Room 2082 is therefore the primary entrance to the office space.

2. **924 Encinitas Boulevard, Apartment 111, Encinitas, California 92024 ("Target Location 2").** Target Location 2 is the Quail Pointe Apartments, located at 924 Encinitas Boulevard, Encinitas, California 92024. The entrance to the apartment is located on the north side of Encinitas Boulevard. Tenant parking is located on either side of road. Building 14 is a two-story, stucco, two-tone apartment complex. The first floor of the building is brown, and the second floor is tan. Apartment 111 is located on the first floor of Building 14. The entrance to the apartment is located on the west side of the building in the north corner. The door is a traditional, non-reinforced metal door. There is no screen door or security door for the apartment. On the north side of the building on the west corner is a patio that is surrounded by a three foot fence and a glass sliding door to the apartment. The patio fence and the trim for the apartment is painted grey. The apartment has two windows. One located to the south/right of the door and one located east/left of the patio doors.



3. 1998 Subaru, California license plate 4STV626, VIN JF1GF4854WG03727 ("Target Location 3"). Target Location 3 is a dark black 1998 Subaru Outback with California license plate number 4STV626, and Vehicle Identification Number (VIN): JF1GF4854WG03727. According to California Department of Motor Vehicles records, Target Location 3 is registered to Richard SILLS, Jr.



ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED

The following items are subject to seizure pursuant to this search warrant:

1. Items potentially used to construct a hoax bomb including but not limited to the following: masking or other types of tape; gloves; wiring such as audio wires with male jacks; propane containers and/or accessories; devices that use propane; any antenna type rod; shotgun shells and/or box; and Coleman camping fuel cylinder;
2. Tools used to construct hoax bomb including but not limited to wire cutters, scissors, razor blades, and/or knives;
3. Items such as books, magazines, articles, photographs, drawings, letters, communications, videos, media, emails, internet research relating to improvised explosive devices (IED), hoax IEDs, bombs, incendiary devices, destructive devices; or any similar device;
4. Firearms or other weapons including 12 gauge shotgun;
5. Items such as books, magazines, articles, photographs, drawings, letters, communications, videos, media, emails, internet research related to Animal Liberation Front (ALF) or animal rights extremism/activism;
6. Items used to create threat letter including but not limited to computers, typewriters, magazines, envelopes, printers, unused bond paper, computer manuals;
7. Digital media devices including, but not limited to, hard disk drives, floppy disks, CDs, DVDs, magnetic tapes, magnetic optical cartridges, personal digital assistants, cellular phones, pagers and memory chips. Cameras, film, digital cameras, memory cards, and thumb drives.
8. Documents exhibiting dominion and control such as utility bills, phone bills, or a lease;
9. Documents relating to the purchase of any IED components including receipts, and credit card bills;

1 10. Phone calls occurring during the course of the search, cell phones and charging
2 equipment.

3 11. In search for data capable of being read, stored or interpreted by computer
4 equipment or storage devices, law enforcement personnel executing this search warrant will
5 employ the following procedures:

- 6 a. The computer equipment and storage devices, including servers may be seized and
7 transported to an appropriate law enforcement laboratory for review. The
8 computer equipment and storage devices will be reviewed by appropriately trained
9 personnel in order to extract and seize any data that falls within the list of items to
10 be seized set forth herein.
- 11 b. In searching the data, the computer personnel may examine all of the data in the
12 computer equipment and storage devices to view their precise contents and
13 determine whether the data falls within the items to be seized as set forth herein.
14 In addition, the computer personnel may search for and attempt to recover
15 "deleted", "hidden" or encrypted data to determine whether the data falls within
16 the list of items to be seized as set forth herein.
- 17 c. If the computer personnel determine that the computer equipment and storage
18 devices are not longer necessary to retrieve and preserve data, and the items are
19 not subject to seizure, the government will return these items within a reasonable
20 period of time not to exceed 30 days from the date of seizure.
- 21
22
23
24
25
26